Hands-On Network Analysis, Troubleshooting and Cyber Crime

Presented by Sunny Connection Instructor: Laura Chappell

Lab List

The following labs are near completion for next week's hands-on analysis class taught by Laura Chappell. Remember to sign up now at http://www.sunny.ch to get a seat!

Application Response Test

Identify and examine the effect network traffic levels have on application performance. Document your results for management.

Proprietary Application Testing

Customize your Application Response Test system to focus on a proprietary application's behavior.

Configure a Remote Analyzer

Set up a remote analyzer station to remotely gather statistics and packets for off-site analysis.

Test Cable Performance

Perform a series of cable tests to identify active pairs, cable shielding levels, crossover faults, impedence issues and more.

Characterize Network Traffic

Examine and document general network characteristics such as broadcast levels, error rates, protocols in use, and packet size distribution.

Identify Application Faults

Isolate the cause of a failing client/server application – is it the cable, protocol stack, NICs, interconnecting devices, server, application, authentication system or some other problem?

Identify a Rogue Application

Use analyzer summary statistics to locate an unwanted application on the network. Build a custom filter to capture this traffic and isolate the source of the traffic.

Convert Trace Files

Capture trace files on one analyzer, convert them to another analyzer format and compare and contrast different decodes.

Sanitize Trace Files

Convert confidential trace file IP addresses to generic private IP addresses.

Build Standard Filters

Set up basic filters to capture traffic based on a port number or IP address.

Build Advanced Filters

Build filters based on binary, hexadecimal, and ASCII values to capture specific traffic on a troubled network.

Study Application Characteristics

Configure an analyzer to track an application from the startup through shutdown process. Identify dependencies and faults.

Catch a Cyber-Thief

Configure an analyzer to capture unwanted traffic that has passed through the firewall – learn to base filters on upper-layer characteristics.

Build a Master Filter Set

Build a set of filters to track the most important and troublesome protocols on a network. Export the filters and take them home!

Check Network Statistics

Identify network problems based on general characteristics and summary data.

Identify Proper Tools

Examine and identify the proper tools to use for various tasks including cable testing, connectivity testing, port scanning, file sanitizing and more.

Test Your Firewall

Set up a firewall test to determine whether specific dangerous ports are truly blocked.

Applications and Tools Used in This Class

Special thanks to the vendors who graciously provided the full working versions of their products to the class participants for in-class use only.

- Sniffer Pro
- EtherPeek for Windows
- Fluke OptiView
- Hex Workshop
- NeoTrace Pro
- NetDoppler
- NetScanTools Pro 2000
- OptiView Remote
- PacketScrubber
- ProConvert
- Sam Spade

Seminar Details

Date: June 27 to 29, 2001
Location: Swissotel Zurich-Oerlikon, Phone +41 1 317 31 11
Time: 9 am to 5 pm
Registration: http://www.sunny.ch

Questions about this class format or structure? Contact us at info@packet-level.com.
Questions about seminar registration? Contact us at info@sunny.ch.